LAW JOURNAL NEWSLETTERS

The Corporate Counsellor

Volume 16, Number 3 August 2001

PROPRIETARY RIGHTS

The Sorry State Of Trade Secret Protection

By R. Mark Halligan and Richard F. Weyand

It's your worst nightmare. Your company's major asset is completely unprotected. Careless or untrained employees are giving it away. Disgruntled ex-employees are stealing it outright. Your competitors are actively engaged in professional and well-directed efforts to take it. It is poorly documented; to the point that you can't even prove it is yours. It is completely uninsured, unaudited and untracked; you don't know what it's worth, or where it is. Your whole corporate culture accepts this state of affairs as its normal business practice.

Then you realize it's not a nightmare, it's true.

Your company's major asset is its confidential and proprietary information, its trade secrets, the knowledge required to run your business every day. More important and more valuable than all the buildings, machines and vehicles, it is irreplaceable. It is the one thing that differentiates you from your competitors and makes you successful.

And the odds are good that it is being stolen as you read this.

The Problem

Trade secrets are rapidly becoming the intellectual property of choice due to their advantages in the information economy. Machinery and mechanisms were the brainchildren of the Industrial

continued on page 7

SECURITIES

Warming Up to Stock Selling Plans: Upholding Rule 10b5-1's Affirmative Defense

By Sean T. Prosser

Maybe it was the declining stock market or maybe the rule was just too new, but many public companies initially were reluctant to encourage their executives to adopt written stock selling plans designed to comport with the defense against insider trading liability created by the new SEC Rule 10b5-1, 17 CFR 240.10b5-1.

To be sure, some executives quickly implemented selling plans, but many others remained hesitant to do so. In fact, some actually rescinded their brand-new plans in the face of declining stock prices and shareholder criticism. Clearly the falling market substantially dampened the initial appeal of such plans. Why would executives want to lock themselves into a selling strategy when prices are so low? Maybe it is a signal of the market turning,, or maybe the passage of time has alleviated concerns, but the number of companies amending their corporate insider trading policies to allow for such plans now is on the rise.

What Is the New Rule?

The affirmative defense against insider trading liability is just a subsection of the new Rule 10b5-1. See Rule 10b5-1(c). Primarily, the rule was the SEC's retort to several court decisions that had held that an insider trading claim is not stated unless it is demonstrated that the defendant actually used nonpublic material information when he or she made an investment decision, rather than the more lenient standard favored by the SEC requiring mere possession of the information. Rule 10b5-1 reflects the SEC's long-held position that insider trading liability arises when a person trades while only "aware" of material nonpublic information. See Rule 10b5-1(b).

Rule 10b5-1 adopts a general rule that any purchase or sale of stock while "aware" of material nonpublic information is illegal, without any need to show that the information was a motivating factor in making the trading decision. See Rule 10b5-1(b). In other words, the rule abolishes any distinction between "use" and "possession" of inside information and increases the risks for executives who sell stock, whatever the reason, at a time when they arguably know material undisclosed information.

continued on page 2

In This Issue

Trade Secrets

continued from page 1

Age, and patent law was designed to protect them. In the Information Age, trade secret protection is better suited to the fast-moving and unpatentable confidential information we need to run our companies. But companies have not yet developed an effective system for realizing the full value of trade secret rights.

The financial risks of loss are large. The Brookings Institution estimates that "at least 50 percent, and possibly as much as 85 percent" of the value of American companies is attributable to intangible assets.[1] This helps explain the large differences between book value and stock market capitalization. The difference represents the valuation the market has placed on intangible assets. If even half of the total market value is attributable to intangible assets, then the value of intangible assets for all publicly held companies in the United States would exceed $6 trillion. And, like tangible assets, directors and officers have a fiduciary obligation to protect these intangible assets.

At the same time that the information economy has made trade secrets more important, it has made them more likely to be stolen. A more mobile work force, increased use of contractors and consultants and increased outsourcing of infrastructure all provide opportunities for trade secret information to leave the company's control. Information technology itself contributes to the mobility of information.

Increasingly, information is stored in easily copied computer files, and Internet connectivity and high-density media such as CD-ROMs make these files easy to transport. A disgruntled employee can literally walk out the door with the company in his pocket.

But the risk of loss is much greater than just from disgruntled employees; any uninformed employee presents a risk. Today, many employees do not recognize that information to which they have access at work qualifies as trade secret information. Well-meaning employees routinely disclose trade secrets to trade show attendees, job candidates, the press and other third parties.

Without any systematic approach to the identification of trade secrets, it is often difficult to draw the line between an employee's general knowledge, skills and experience on the one hand, and the company's legitimate trade secret rights on the other. Many employees believe that they own all the work product of their efforts. This is a common point of view among technology professionals today.

The Law

The modern definition of trade secret encompasses any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.[2]

The law provides protection for trade secrets if certain legal requirements are met.[3] However, unlike patents, copyrights and trademarks, there is no office or agency where you can file a trade secret application, obtain a review by a qualified examiner and be issued an official trade secret certificate.

The legal protection of trade secrets instead requires self-administration by the trade secret owner. Traditionally, the intellectual property bar has recommended trade secret audits.[4] However, trade secret audits are expensive, and most companies do not spend the money to conduct them. Further, trade secret audits are only "snapshots" at a given point in time. The trade secret status of information assets is constantly changing and the results of trade secret audits can become quickly outdated.

At the present time, most companies wait until their trade secrets have been compromised, and then file suit for trade secret misappropriation. It is only then that trade secret rights are identified and protected. However, it is often too late to protect trade secrets at this stage. It is difficult, after the fact, to go back and prove the existence of a trade secret. Employees have retired or are deceased, memories have faded, documents no longer exist or cannot be found.

A trade secrets audit conducted during litigation is haphazard at best. Under the pressure of discovery deadlines, outside counsel scrambles to interview available witnesses and review mounds of documents to identify the trade secrets allegedly taken by the former employee. Under these circumstances, the company often loses the lawsuit. Identifying trade secrets after the fact often reveals a lack of reasonable measures to protect the trade secrets or any evidence that the employee even had access to them. Courts often take exception to imposing liability on a former employee for trade secret misappropriation when the company did not treat the information as a trade secret in the first instance.

And trade secrets, once lost, are lost forever.[5]

The Solution

Trade secrets require identification and protection. The starting point of any solution must therefore be an ongoing accounting system for trade secrets. A company must first know what they are and where they are located. The law has established a six-factor test for the identification of trade secrets that provides the benchmarks necessary for assisting a company in identifying trade secret assets.[6] These six factors are as follows:

Factor 1: The extent to which the information is known outside the company. The more extensively the information is known outside the company, the less likely it is a protectable trade secret.

Factor 2: The extent to which the information is known by

continued on page 8

R. Mark Halligan is a principal in the Chicago intellectual property firm of Welsh & Katz, Ltd. and a nationally recognized expert on trade secrets law (*www.rmarkhalligan.com*). **Richard F. Weyand** is president of The Trade Secret Office Inc. (*www.theTSO.com*). They are co-inventors of a patent-pending accounting system for the identification and protection of trade secrets called the Trade Secret Examiner.

Trade Secrets

continued from page 7

employees and others involved in the company. The greater the number of employees who know the information, the less likely it is a protectable trade secret.

Factor 3: The extent of measures taken by the company to guard the secrecy of the information. The greater the security measures, the more likely it is a protectable trade secret.

Factor 4: The value of the information to the company and its competitors. The greater the value of the information to the company and to its competitors, the more likely it is a protectable trade secret.

Factor 5: The amount of time, effort and money expended by the company in developing the information. The more time, effort and money expended by the company in developing the information, the more likely it is a protectable trade secret.

Factor 6: The ease or difficulty with which the information could be properly acquired or duplicated by others. The easier it is to duplicate the information, the less likely it is a protectable trade secret.

Applying these six factors, companies can identify trade secrets in advance of litigation, and then take the necessary steps to ensure that sufficient documentation is in place to identify these assets and that reasonable measures are in place to protect them.

This identification and protection of trade secrets is an ongoing and continuous process. An effective program requires the continuous classification of new trade secrets and the declassification of stale trade secrets that no longer have economic value.

Employee education must be an integral part of any trade secret protection plan. Employees must be made aware of their fiduciary duty to protect confidential information and periodically warned about situations that may result in the inadvertent loss of trade secrets. Processes must be in place for notifying employees of the company's trade secret rights and for protecting trade secrets as they are used in the company's business operations.

Finally, access to trade secret information must be tracked. Trade secrets should be disclosed internally only on a "need to know" basis. The emerging trend of posting confidential information on the company's internal web site—for all to see—is contrary to effective trade secret protection. The more people who have access to the information, the less likely the information will qualify as a trade secret.[7] Access to trade secret information should be strictly controlled, and access should be tracked so that the company can win the trade secret lawsuit against a former employee who denies knowledge of the trade secret in litigation.

The time has come to develop an effective accounting system for intangible trade secret assets. The identification and protection of trade secret assets can no longer be ignored until a trade secret misappropriation lawsuit is filed. Officers and directors have a fiduciary duty to identify these assets in the new economy; only then can these assets be effectively insured, valuated, licensed and protected. And only then will companies realize the full potential of the information economy and correct the current sorry state of trade secret protection.

---

(1) "New Ways Needed to Assess New Economy," Margaret Blair, Brookings Institution, Nonresident Senior Fellow, Economic Studies, in The Los Angeles Times, Nov. 13, 2000.

(2) See Restatement of the Law (Third) Unfair Competition § 39 (1995).

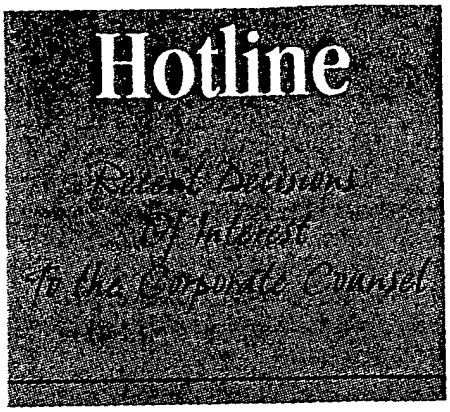
(3) The two primary requirements are (1) that the information not be generally known in the trade, and (2) that the trade secret holder take reasonable measures under the circumstances to protect the information as a trade secret. See generally, Uniform Trade Secrets Act, § 1(4) (definition of a "trade secret").

(4) See, e.g., R. Mark Halligan, Trade Secret Audits, *www.execpc.com/~mhallign/tradesec.html*

(5) *FMC Corp. v. Taiwan Tainan Giant Industrial Co.*, 750 F.2d 61, 63 (2d Cir. 1984).

(6) Restatement (First) of Torts § 757 (1939).

(7) "[T]he extent of a property right [in a trade secret] is determined by the extent to which the owner of the secret protects his interest from disclosure to others." *Ruckelhaus v. Monsanto*, 476 U.S. 986, 104 S.Ct. 2862 (1984).



ATTORNEY FEES

Rejection of Rule 68 Settlement Offer Limits Fees Plaintiff May Recover

The U.S. District Court for the Eastern District of Pennsylvania has ruled that a plaintiff in an employment discrimination suit is not entitled to attorney fees for work done after a formal pre-trial settlement offer is made, even if it is rejected by the plaintiff and followed by a jury award that is less than the defendant's offer. *Tai Van Le v. University of Pennsylvania*, No. CV. A. 99-1708 (July 13).

The plaintiff was an electronics engineer who filed suit against his employer claiming that he was fired for complaining about national origin harassment he received. At trial, a jury rejected his harassment claim but found the plaintiff had been the victim of retaliation and awarded him $25,000 in compensatory damages and $10,000 in punitive damages. Prior to trial, the plaintiff had rejected a settlement offer of $50,000 made pursuant to Rule 68 of the Federal Rules of Civil Procedure. Following the trial, the defense filed a post-trial motion seeking all costs it had incurred after making the settlement offer, as well as the attorney fees that were incurred in taking the case to trial. The plaintiff argued that the defense was not entitled to any fees or costs since the verdict, combined with the fees incurred up to the date of the offer, totaled more than $50,000.

The district court found that the plaintiff had to reimburse the defendant for any costs incurred after the formal offer was made, but that the defendant was not entitled to recover attorney fees for taking the case to trial. The court stated that while the U.S. Court of Appeals for the Third Circuit had never addressed this issue, several district courts within the circuit had, and they ruled that Rule 68 does not entitle the defense to any attorney fees. The